ICS 153

Introduction to Computer Networks

Inst: Chris Davison

cbdaviso@uci.edu

ICS 153
Application Layer

- Contents:
  - Network Security
  - Domain Name System (DNS)
  - Simple Network Management Protocol (SNMP)

Network Security

- Network security is a broad topic that may cover:
  - Risk Assessment
  - Asset Valuation
  - Policy Formation and Implementation
  - Auditing and Incident Response
- A computer network is secure if you can depend on it and its software to behave as you expect.

Network Security

- Four areas of Network Security:
  - Secrecy
  - Authentication
  - Nonrepudiation
  - Integrity Control
- Every layer can contribute to network security.
  - Application Layer: PGP
  - Physical Layer: special transmission lines

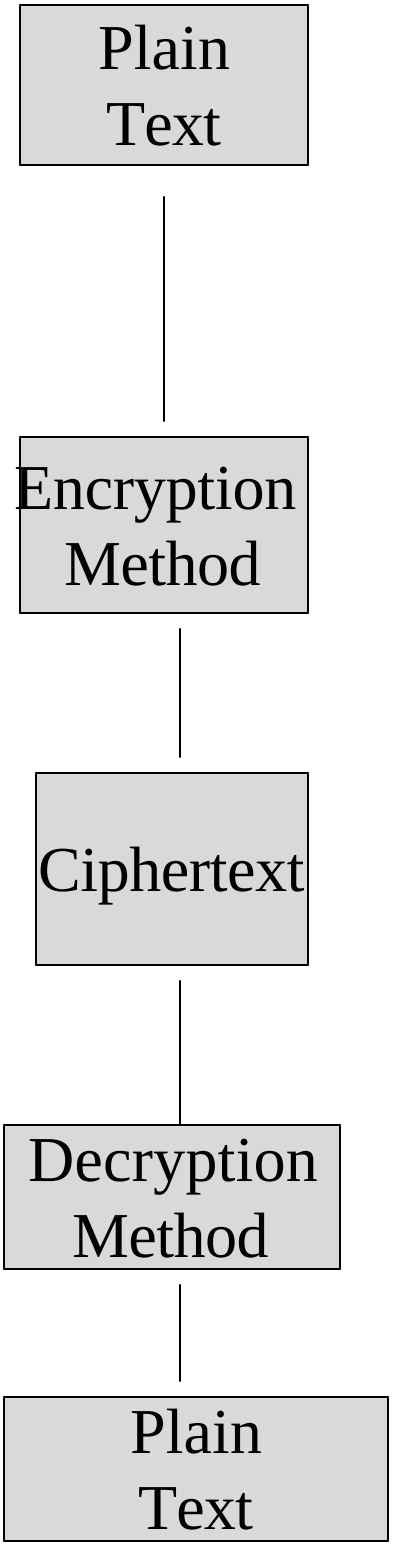
Network Security
Secrecy

- Secrecy pertains to keeping information out of the hands of unauthorized users.
  - Physical Security
    - Locks, vaults, guards
  - Cryptography

Cryptography Definitions

- Cryptanalysis
  - Art of breaking ciphers
- Cryptography
  - Art of devising ciphers
- Cryptology
  - Study of cryptanalysis and cryptography
- Private Key Cryptography
  - Uses the same key to encrypt and decrypt. Key must be kept secret
- Public Key Cryptography
  - Uses a public key to encrypt and a private key to decrypt. Only the private key is kept

Encryption Model



Private Key Encryption Methods

- Substitution Cipher
  - Each letter or groups of letters is replaced by another letter or group of letters.
  - Caesar Cipher
    - Used by Caesar's troops
  - Rot13
    - Usenet method of encryption
- Easily broken

Private Key Encryption Methods

- Transposition Ciphers
  - Reorder letters but do not disguise them
  - Columnar cipher
    - Plaintext is encrypted in columns based on a keyword
- Not as easy to break as the Substitution Cipher

Private Key Encryption Methods

- One-Time Pads
  - Ciphertext is created by converting the plain text into a bit string and XORing it with a random bit string key.
- Unbreakable Cipher
- Key is almost impossible to memorize
  - Sender and receiver must carry a copy with them

Private Key Encryption Methods

- DES
  - Data Encryption System
- An encryption algorithm developed in the 1970s by the National Bureau of Standards and Technology and IBM.
- Uses a 56-bit key and 19 distinct encryption stages.
- Very strong but breakable

Private Key Encryption Methods

- IDEA
  - International Data Encryption Algorithm
- Published in 1990
- Uses a 128-bit key
- Very strong encryption algorithm, no practical attacks have been published.
  - “brute force” attack not practical
- Covered under various International Patents

Private Key Encryption Methods

- Skipjack
  - Classified (SECRET) algorithm developed by the NSA.
  - Algorithm used by the Clipper encryption chip
  - Utilizes an 80-bit key

Public Key Encryption Methods

- RSA
  - Created by: Rivest, Shamir, Adlemin 1978
- Very strong encryption
  - Supports variable length keys
  - Longer keys provide more security
- Algorithm is based on Prime Number computations.

Authentication

- Authentication is the technique by which a process verifies that its communication partner is who it is supposed to be and not an imposter.

Authentication

- Three ways to authenticate:
  - Tell the host something you know:
    - password (shared secret key)
  - Show the host something you have:
    - Card key
  - Let the host measure something about you:
    - Fingerprint

Digital Signatures

- Guarantee the authenticity of the “digitally signed” message
- A digital signature is encrypted with someone’s private key to certify the contents:
  - authenticity
  - integrity
  - against repudiation

Digital Signatures

- Secret-Key Signatures
  - A central authority is used as a repository for all digital signatures.
  - Everyone must trust the central authority.
- Public-Key Signatures
  - Encrypt a messages with the sender's public key and decrypted with the sender's private key

DNS

- Domain Name System
  - RFCs 1034 and 1035
  - Hierarchical, domain-based naming scheme and a distributed database system system for implementation
  - Used for mapping host names and email destinations to IP addresses
  - Port 53

DNS

- Internet is divided into a hierarchy with several hundred top level *Domains.*
  - com
  - gov
  - edu
- Domains are further divided into sub-domains.
  - Each domain controls how it allocates domains under itself.

DNS Resource Records

- Set of records containing the information that a domain is responsible for.

- Resource records can track the following information:
  - IP addresses (A record)
  - mail exchange information
  - aliases
  - machine names (Cname record)

DNS
Name Servers

- For efficiency, the DNS name space is divided into many, non-overlapping zones.
- Each zone has an authoritative name server that manages and answers queries for the zone.

SNMP

- Simple Network Management Protocol
  - RFC 1157 (SNMP 1)
  - RFCs 1902-1908 (SNMP2)

SNMP Model

- SNMP model consists of four components:
  - Managed nodes
    - hosts, routers, etc.
    - Must run the SNMP management process known as the *agent*
  - Management stations
    - Computers running the SNMP management software
  - Management Information
    - *Objects* (variables) contain state information
  - Management Protocol
    - SNMP protocol used for communication
    - Port 161

SNMP Data Structures

- SNMP data structures are defined by Structure of Management Information (SMI)
  - An Abstract Syntax Notation One (ASN.1) derivative

Management Information Base

- The collection of all possible objects (175) in a network is given in a data structure called the Management Information Base (MIB)
  - Grouped into 10 categories